DO'S, DON'TS, AND RECOMMENDATIONS

The following guidelines are "Lessons Learned" to follow when designing applications. The guidelines are based on the Applications Lab experience in dealing with GOTS applications in the NMCI Environment. These guidelines are intended to improve the standardization of GOTS applications, with the following benefits:

- Increase the application compatibility within the NMCI environment
- Facilitate enterprise packaging
- Reduce certification processing and troubleshooting time

Standardization is organized into three categories:

- Do's
- Don'ts
- Recommendations

Do's

The following guidelines significantly reduce the turnaround time of Packaging and Certification.

- Place the applications into the C:\Program Files\Application Name folder, where Application Name is the name of the program.

  EXAMPLE: Place the applications into C:\Program Files\USN AMP, where "United States Navy Aircraft Maintenance Program" is shortened to USN AMP. Support files may be installed to other locations, but the main application must be installed in the Program Files\USN AMP folder.

- Store temporary files in the C:\Program Files\Application Name\Temp folder.

  Temp files are commonly stored in the C:\Temp folder. The folder is not supported in the NMCI environment due to its use of the enterprise software distribution system. Temporary files must reside in a location that users have NTFS write or modify permissions. The "Temp Folder" inside the application folder allows EDS personnel to quickly identify temporary files when troubleshooting.

  EXAMPLE: "C:\Program Files\USN AMP\Temp"

- Store configuration files (e.g., ini, cfg, sys, etc.) in one of two locations depending on level of the file protection/permission.

  Locating files in one of these two locations allows EDS personnel to quickly process applications for Packaging and Certification.

- Store files that are to be updated in the C:\Program Files\Application Name\Config folder.

    EXAMPLE: "C:\Program Files\USN AMP\config.cfg" (modifiable at runtime)

- Store files that are not to be modified in the C:\WINNT\System32\Developer\Application Name

    NOTE: This is for files that are not to be modified.

    EXAMPLE: C:\WINNT\System32\Developer\USN AMP\config.cfg" (not modifiable at runtime)

- Store data files (including saved data files and databases) either on the Local Machine or in a shared folder in the network.

    – Local Machines:

        o **Single User:** Only one specific user may store and use these files. Store these files in the "C:\Documents and Settings\username\My Documents" folder.

            EXAMPLE: C:\Documents and Settings\username\My Documents\USN AMP\Data

        o **Multiple Users:** More than one person may use these files, which usually serve as a common source of data. Locate these files in the "C:\Program Files\Application Name\Data" folder.

            This allows EDS personnel to know where the application data files are stored and take proper measures to prevent those files from being updated or overwritten by the enterprise packaging system.

            EXAMPLE: "C:\Program Files\USN AMP\Data"

    – **Shared Folders:** Use any shared path as long as the UNC discussed in this document is adhered to.

        EXAMPLE: "\\SPAWAR\SPOT\CMDSHARE\USN AMP\DATA"

- Install Application Shortcuts to the "C:\Documents and Settings\All Users\Start Menu\Programs\Application Name" folder.

    This ensures that the shortcuts are created in the Start Menu for all users and standardizes the location of shortcuts. If an installation package that installs shortcuts is used, care should be taken to ensure that only the "All Users" Start Menu shortcut is used.

    EXAMPLE: "C:\Documents and Settings\All Users\Start Menu\Programs\USN AMP\USN AMP.lnk"

- Provide test data with a test plan for an application if data files (such as databases) are used.

  This allows for EDS personnel to conduct tests and verify that the program is functioning correctly.

- Validate .msi package files using a test program, such as ORCA.

  The enterprise packaging system is not capable of validating MS Windows Installer (.msi)-based applications.

- Create a login account and a password for testing applications that require the use of a login.

  If a login account has not been provided testing applications that require the use of a login, the Applications Lab will reject the application because the certification test cannot be performed.

- Provide License and/or Registration keys if required by the application.

  Without License and/or Registration keys keys, the Applications Lab will reject the application, because the certification test cannot be performed.

- Completely fill out a RFS form for each application.

  See instructions for this form in the ISF Tools Database Users Guide on the ISF Tools Database Log-in page.

  The listed POC should be someone highly familiar with all aspects of the application.

- Provide a copy of the application manual or documentation to ISF personnel on how to perform the following actions:

  – Install the application.
  – Test the application.
  – Operate the program.

- Provide an abstract (overview) on the purpose and use of the application.

- Provide information (release notes) on known or acceptable errors and bugs.

  Any undocumented error that EDS personnel cannot solve will cause the Applications Lab to reject the application.

- Ship the applications on 3.5" floppy diskettes or CDs.

Don'ts

This section lists items that will cause the Applications Lab to reject applications, or require substantial increased processing and turnaround time for application certification. The Applications Lab strongly recommends following this list to avoid immediate rejections and shorten the time for certification.

- Do not use desktop shortcuts (shortcuts that are on a user's desktop screen). Desktop shortcuts created from applications are kept to a minimum in the NMCI environment. Users are allowed to create shortcuts themselves.

- Do not compress or zip the preinstalled application. Applications should be installed from diskette(s) or CD(s) without the need to uncompress or unzip. This is because machines used to package the application for enterprise deployment are not able to uncompress or unzip.

- Do not use the term "Beta" for versioning. An application that contains "Beta" in its version is automatically rejected, as this application is assumed to be a preproduction version.

  EXAMPLE: Use the numeric format for versioning (i.e., 2.00.2), instead of words (i.e., 2.00 Beta).

- Do not use modems. Do not include any functionality that requires the use of a modem.

- Do not use "Uninstall" or "Rollback" scripting in the installation executable files. The NMCI enterprise application management system performs uninstall and rollback.

- Do not duplicate any Gold Disk applications or their functionality within any release: http://www.nmci-eds.com/downloads/Gold_disk_contents.pdf.

Recommendations

The Applications Lab provides the following tips to allow for quick certification, ease of troubleshooting and updating.

- Use good design standards and practices for programming.

- Provide as much clear information about the application as possible. More information means easier certification.

- Prepare application configuration files in text format. Text-based configuration files allow for quick turnarounds in reconfiguring without complete repackaging of the application for enterprise deployment.

  EXAMPLE: An application designed for use at NAS Pax River is requested for use at NAS Lemoore, and is configured on a network. If the application uses a text-based configuration file, the Applications Lab can make the changes needed to the file within

the NAS Pax River package without having to repackage and test the application. If the application has hard coded, embedded or encrypted files in the application, the program must be completely repackaged and certified.

- Minimize the use of large application on local workstations. (The developer must determine what is a "small" or "large" application) For a large application, two possible solutions may be used:

  - Use servers to support large programs or files (preferred solution).

    For example, a local workstation (front end) has a small program to allow a user to use the large database (back end) off a server.

  - Use CDs from a CD library (where possible) or on local workstations (least preferred).

- Review the latest Group Policy Object (GPO) revisions. Obtain the GPO information from the NMCI DAA.

- Schedule and coordinate the testing of application releases with Applications Lab personnel to allow developer participation in the Packaging and Certification process.